EHR REPORT

A Legal Take on the Audit Trail

BY AMY A. QUINLAN, RICHARD GALPERIN, AND NEIL SKOLNIK, M.D.

(This is the first part of a two-part series.)

Electronic records have many benefits; however, health care providers should be aware that electronic health record systems can increase exposure to legal liability and medical malpractice in ways defined and yet to be defined.

The potential impact of EHRs on the medical-legal system is large, and courts around the country are scrambling to make sense of how EHRs affect information flow, access, and liability. What information must be produced, and whether the information is admissible in court, are two important questions that have begun to surface. Plaintiff attorneys are beginning to tap into the array of information available in an EHR.

An important area of increased attention and exposure is the access control, or audit trail function, of EHR systems. In this first part of a two-part series, we will consider the increased legal risks and benefits to physicians brought about by EHRs, focusing on the audit trail.

What Is an Audit Trail?

The audit trail is a record of all access to the electronic medical record and supports the legal integrity of the records by creating a system that establishes accountability for activities. Before the EHR, access to the paper medical record was tracked through the use of a sign-out sheet, a log book, or often no tracking system at all.

EHRs have far greater potential for auditing and record verification. The health care provider must appreciate that each time she accesses a patient's medical records, she is leaving an indelible track of her access. To the extent that courts deem audit trail records admissible, juries will see your contact with the patient's charts as clear as footsteps in wet cement—and as permanently preserved. Discovery rules are just starting to change to address electronic discovery, including EHRs.

To add to the confusion, not all systems are created equal. For instance, some systems offer the ability to track the specific record accessed, and some do not. Others have the option to turn off the audit trail functionality or provide override features. Questions arise around the protection of access numbers and the reliability of the manner in which a system tracks an individual provider.

The extent to which a system protects this information is critical in the medical-legal context, because these issues can affect the admissibility of such information at trial.

The Trail Wagging the Dog

With a robust audit trail function in place, information never before available may provide fodder for the savvy litigant. This information has the potential to shift the standard of care.

For example, the ability for a hospitalist to review all prior hospitalizations might be difficult with a paper record, but may not be so difficult with an EHR—thus making a new standard of complete review of the readily available records. Another question that may arise: How quickly must a physician review test results if a system is in place that allows immediate access?

Conversely, the EHR could be helpful in corroborating a health care provider's testimony that the specific information was not available at the time that a decision was made.

How and where a health care provider has accessed the EHR is an issue emerging in medical malpractice actions. Electronic records provide the ability to trace the date and time a provider accessed the system, how often the information was accessed, and, in some instances, from where access was acquired and what documents were reviewed. This information, never before available, complicates what lawyers refer to as e-discovery, making a physician's office and home computer, laptop, or other electronic device susceptible to requests for production.

Questions regarding the admissibility of e-mail, cell phones, iPads, notebooks, and other PDA devices are all up for grabs. EHRs provide access to much more information than previously available and will likely add to increased legal costs and case complexity.

Avoiding Legal Exposure

► Protect your identification code. Because access to the records is tracked through the use of identification codes, protecting that code to prevent unauthorized access is critical.

► Do not share your code. It can be problematic when a physician allows members of her staff access to her code. This makes it difficult at a later date, during litigation, to determine who accessed the medical chart. Individual separate identification codes should be given to each staff member in your office who may need to access the EHR.

► Sign out whenever possible from shared computer terminals. This minimizes the risk that someone else will access a record, with it appearing that it was you.

► Understand the consequences of a decision to access a record or not.

► Consider making a written note in the patient's chart of any significant information learned from your access.

► After an unexpected outcome, think carefully before you access the chart. If you are not accessing the chart for ongoing patient care reasons, you may later need to explain your chart review.

► Once engaged in litigation, before your giving testimony, learn what auditing was done of the chart by you and others. This will help avoid potential contradictory testimony.

More to Come

In our next column, we will discuss two real-world scenarios that illustrate the potential benefits and risks to the malpractice litigant, and the importance of maintaining the integrity of the EHR for litigation purposes. ■

MS. QUINLAN is an associate and MR. GALPERIN is a partner at Morris James Delaware. DR. SKOLNIK is associate director of the family medicine residency program at Abington (Pa.) Memorial Hospital, professor of family and community medicine at Temple University, Philadelphia, and editor of the recently published "Electronic Medical Records: A Practical Guide for Primary Care" (Humana Press, 2010).

HHS Proposal Would Tighten Health Privacy Requirements

BY MARY ELLEN SCHNEIDER

Patients could gain greater access to their health information and have more power to limit disclosures of certain personal information to health plans under a new proposal from the Health and Human Services department.

The new requirements, which were announced in July, are aimed at beefing up privacy and security, as the Obama administration pushes to get more physicians using electronic health records over the next few years.

"The benefits of health IT can only be fully realized if patients and providers are confident that electronic health information is kept private and secure at all times," Georgina Verdugo, director of the HHS Office for Civil Rights, said in a statement. "This proposed rule strengthens the privacy and security of health information, and is an integral piece of the administration's efforts to broaden the use of health information technology in health care today."

The proposal alters the Health Insurance Portability and Accountability Act (HIPAA) rules by setting new limits on the use of disclosure of protected health information for marketing and fundraising and by requiring business associates of HIPAA-covered entities to follow most of the same rules that covered entities follow.

The proposal would also bar the sale of protected health information without explicit authorization from the patient.

The proposal also implements elements of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, which requires physicians and other covered entities to grant patient requests to restrict certain information from their health plans.

For example, the proposed rule states that patients must be allowed to restrict protected health information if that information is related only to a service for which the patient paid in full and the information is not otherwise required by law to be reported.

Individuals can provide comments on the rule for a period of 60 days, which began on July 14. Along with the release of the proposed regulation, HHS has also launched a new Web site (http://www.hhs.gov/healthprivacy/index.html) that provides consumers with information on their privacy rights under the existing regulations. ■